Disaster Recovery and Contingency Planning

Overview

Lore Systems' approach to continuity planning and disaster recovery is to prevent avoidable instances of unplanned interruptions and to minimize the impact of events that cannot be avoided. Disaster avoidance is built into our Tier 3 facilities. The purpose of a disaster avoidance system is to detect certain problems, and respond to them, before they develop into unplanned interruptions. This includes not only infrastructure systems such as physical security, fire detection, uninterruptible power systems, structural reinforcement of the building, but also staff training and good housekeeping practices to avoid human errors. Fail over redundancy is built into all major systems within the center.

Lore datacenters are designed to be fault-tolerant, but if a disaster cannot be avoided, we staff our datacenters 24 hours a day, 365 days a year to respond to the unexpected. Tools and spare parts are available to quickly replace failed pieces of the datacenter infrastructure. National support contracts are maintained with suppliers for immediate response. Most importantly, if the unexpected does happened, Lore's philosophy is to keep our customers informed at every step.

Finally, while our disaster recovery planning focuses on the physical infrastructure of our datacenters, some events can only be avoided by geographic diversity. As part of any customer's disaster contingency planning, a customer should also consider computer and network security systems as well as data backup and restoration in case of a catastrophic event. Lore Systems, with its partners, can work with a customer to implement disaster recovery and backup contingencies across multiple centers.

Lore has developed a comprehensive internal Standard Operating Procedures (SOP) for responding to emergencies. In the event of an emergency, catastrophic or otherwise, our staff is trained to quickly respond on all levels of the operation to secure the physical plant, ensure the personal safety of customers and staff within the facilities, and protect the physical equipment and digital assets of our customers. These procedures include:

-Incident Definitions and Condition Codes
-HQ Communications
-Notification Matrix
-Emergency Contact List
-Lore Systems Response Center Processes
-Post-Incident Review/Resolution Tracking
-Government/Safety Entities
-Established Customers
-Non-Customers

External Communication Guidelines

- Evacuation Procedures
- Bomb Threats
- Earthquakes
- Fires
- Flood
- Medical Emergencies
- Other Disasters

In addition to these SOPs for Emergency Procedures, it is important to note, on a proactive nature, that Lore facilities comply with all federal, state, and local municipality codes, regulations, and requirements. This compliance includes all appropriate and applicable occupational safety and health standards as regulated in the OSH Act of 1970.

Emergency Procedures Testing

Lore Systems conducts regular tests/audits on the various components of the datacenter's Emergency Procedures. These tests include a focus on the following:

Power

- Critical Electrical System Maintenance (CESM)

- Backup Generators

Local Emergency Agency Response

Part of our ability to implement our recovery and continuity planning is dependent on how quickly our local emergency agencies can respond in the event of an emergency. We invite local emergency agencies into our facilities for a full physical tour. We go to great length to educate these professionals as to the critical nature of our business and the value of our customer's digital operations. In coordination with this education effort, we also conduct "no-warning" tests to measure response times and appropriately account for these in our Standard Operating Procedures.

Evacuation

Lore's datacenter conducts regular evacuation tests to insure staff compliance and familiarity with documented SOPs.

Fire Suppression

Our facilities are protected with a dual-alarmed, dual-interlock, multi-zoned, dry-pipe, water-based fire suppression system armed with sensory mechanisms (HSSD) to sample the air and give alarms prior to pressurization. Production area fire suppression is provided by a multi-zoned, pre-action, dry-pipe system. In order for the system to trip, multiple cross-linked events must occur. These include detection by ceiling mounted smoke-heads and smoke "sniffers" located throughout the facility. Lastly a sprinkler head must trip in order for the dry-pipe system to activate. This requires a temperature of 140 degrees F at the head location. Fire suppression is localized at the event point only.

HVAC

Our datacenters' HVAC systems are designed to achieve N+1 redundancy and supply enough cooling to support a minimum of 5,968 BTU's per equipment rack. The HVAC delivery system includes redundant water chillers, redundant pump systems, and multiple Computer Room Liebert AC units. As normal raised floors are not permitted within the facilities, air conditioning is supplied via a downdraft from overhead ducts suspended from the ceiling. The air merges through directional vents. The air conditioning management systems are designed to maintain the environment between 68° and 72° Fahrenheit in the server area (+/-2° Fahrenheit).

Comprehensive maintenance and testing of all Systems, including thorough testing of the HVAC systems is conducted. Included with the previously mentioned CESM testing process, Lore Systems performs both preventive maintenance (PM) and predictive maintenance (PdM) on our HVAC systems. Elements include:

- PM scheduling and tracking, our computerized maintenance management system (CMMS).

- ALL maintenance on critical facility infrastructure systems is fully scripted (detailed step-by-step).

- Experienced corporate engineers review ALL scripts prior to the work being done. Customers are advised in advance of critical maintenance activities.

HVAC systems are connected to the electrical busses that receive power from the utility or the generator. The HVAC system is not backed up by the UPS, so if there is a transfer of power between the utility and the generator, the HVAC system may experience a 10 second outage, which is the time it takes for the generators to take over full electrical load. The HVAC delivery system includes two water chillers, redundant pump systems, and multiple Computer Room AC units.

Maintenance

The Lore Systems Critical Maintenance Process includes steps for advance notification of customers, datacenter management, and datacenter staff regarding critical maintenance activities.

Critical Maintenance is defined as any maintenance activity performed on critical infrastructure systems that include all MEP, fire suppression and security systems. Lore recognizes that this activity must be well planned and properly executed to minimize

the possibility of interruption of service to customers. The process must be strictly followed for coordination, documentation and performance of critical maintenance.

Lore always notifies customers via email of any maintenance performed.

The datacenter performs "hot" work, or comprehensive maintenance and testing of all Electrical Systems in a process referred to as CESM. This includes Utility, Generator, UPS and -48VDC Distribution.

Backup generators are tested weekly, monthly (full load condition testing), quarterly, and annually, with all major components of the generator systems.

A master schedule for critical maintenance activities (e.g. UPS systems, generator, and battery maintenance) is used. The master schedule is used to assure proper planning of critical maintenance activities.

All critical electrical switching activities are fully scripted. Each step is planned, documented and reviewed by engineering management to assure accuracy and safety.

As an integral part of ongoing maintenance for our Customers' operations, Lore maintains a comprehensive and automated process responding to alarms or service requests and an aggressive escalation and notification plan that keeps our Customers Operation's Management informed of resolution progress at all times. There are four (4) levels of priority assigned to all ticket items, whether a routine service request, or an activated alarm. A Time to Resolution Goal is established for all tickets based on assigned priority. Customers can independently assign a severity code (Normal – High – Critical) to all tickets that may impact resolution timeline goals as stated in service level agreements. Escalation begins after documented Resolution Time goal is in jeopardy. Customer provides three (3) levels of Emergency Contacts during the fulfillment process.

Lore Systems plans, monitors, records, maintains, troubleshoots and resolves all incidents that involve the availability of Cage Space, Power, IP connectivity or Additional Services it provides. Trouble Reporting and Escalation is provided through our response center and process. This is available 24x7, 365 days a year. Customers can telephone us directly or interact with us via our secure Web portal.

Systems

Power (General Description)

Each major component within our facilities is designed to be N+1 redundant. The fully redundant N+1 design is modular in nature, meaning that additional power system modules (battery strings, UPS modules, generators, etc.) can be added into the existing system should it become necessary to do so in order to maintain full redundancy. All power system components are monitored through an Automated Logic Control System (ALCS). With the ALCS, the facility engineering team can monitor all components of power, HVAC and emergency support systems from within the IBX or from a remote location.

DC/AC Power Generation and Distribution

Conditioned AC and DC power, with two independent A & B power buses respectively are available to customers. UPS, battery and diesel generators back up every datacenter power system. Each center has redundant 1500KW Caterpillar diesel generators as well as refueling contracts to be delivered within 24-hours, when fuel tanks have 75% capacity.

CESM

As required, a comprehensive maintenance and testing of all Electrical Systems in a process referred to as CESM is conducted. This includes Utility, Generator, UPS and 48V DC Distribution.

There are a number of reasons to organize and structure these events. Lore Systems is not the originator of this maintenance process. Major financial, military and other datacenters have used this process for nearly 20 years. Our partner Equinix has extracted the most beneficial aspects of procedures used elsewhere and streamlined the "Powerdown" activity into our CESM. Here are some benefits of performing our CESM over having contractors simply perform contract maintenance.

Left to perform maintenance independently of each other, contractors address their systems as one system. The CESM process maintains and tests the electrical distribution as a single system, interconnected with various sub-systems.

Reduced Exposure: For instance, rather than taking down a UPS System once for Switchboard maintenance and again for UPS maintenance, CESM takes it down one time for both efforts.

- CESM affords a co-ordination of all maintenance efforts with a minimum of Power-down time.

- Documentation of procedures (Script). These procedures become standardized and may be extracted from electronic records.

- Documentation of issues. Operations staff familiarity training and system interaction. Risk mitigation: Critical evolutions and procedures are planned with a larger number of participants, bringing more expertise into each effort. Additionally, reducing the number of switching exercises minimizes risk of interruption to customers.

- Maximizing the effort from each vendor, by scripting and supervising their participation.

- Team approach: when contractors work with each other, issues not previously considered frequently are identified.

- Mandated testing: UPS Certification (Step Loading, Full Load tests, Transient tests, UPS Thermographic survey) is a Lore Systems procedure, which go beyond typical UPS vendor annual service. Similarly, Paralleling Switchgear Control Failure Tests and "Pull the Plug Tests" are not performed by any single support vendor.

- Change Control / Customer Notification and Marketing: The ERC notifies the Customer of these efforts not less than 30 days prior to the event. This notification is an indication to our customers of how our most critical systems are maintained in a well-planned and systematic manner.

- Facilitating Projects: Projects such as the MSB Power Quality Monitoring installation may be incorporated in the CESM, resulting in reduced cost and minimized system Powerdowns.

- Exercising Devices: The failure of a Circuit Breaker or Switch to operate frequently may be attributed to that device not being exercised. CESM operates every major distribution STS, Switch and Breaker in the datacenter.

- Cleaning: Dust and debris is a major contributor to electrical equipment failures (referenced in IEEE 493). This is especially true of transformers and switches. While it is a

sound practice normally, it is especially needed following construction.

- Branch Circuit current readings. This information is essential to both Lore Systems Operations and Design. Because of the resources required to accomplish this, and the exposure of removing the panel boards while energized, it is performed only twice annually. One of these is during the CESM IR Scan of the panel boards.

- Compliance with Electrical Maintenance Standards in IEEE493 and NFPA 70B.

The following parties/organizations participate in the CESM:

Sigma Six Solutions, an external independent vendor, is an integral member of the CESM Team. They assist in the planning and scripting as well as perform most of the tests and frequently make repairs. They also provide Technical expertise in nearly all electrical arenas, including NEC and IEEE issues, Circuit Breakers, ATS's, ASTS's, Switches, Transformers, Grounding and UPS. They are highly regarded and sought after within our industry and are capable of many functions other testing firms are not. Sigma Six is familiar with our processes and procedures, including CMR, Lockout/Tagout/Switching and Scripting. They have written Scripts and performed work at the facility.

Liebert is responsible for many of the most critical systems within the site. Because of the increased visibility of the CESM effort, Engineers and Management become involved in our annual CESM.

Electrical Contractors: Each Site Manager and Chief Engineer have identified the Electrical Contractor that best serves the needs of that site. Site and System familiarity, competence and cost are factors considered in their selection. This contractor is used to assist with panel removal/reinstallation, Breaker removal, repairs, backfeeding and more.

Beyond the CESM process, performs both preventive maintenance (PM) and predictive maintenance (PdM) on the electrical systems are conducted.

Elements include:

- PM scheduling and tracking, our computerized maintenance management system (CMMS).

- PdM techniques such as battery health analysis using our BTech battery monitoring systems, oil analysis on engine-generator systems, and annual infrared scanning of all distribution panelboards and switchgear.

- ALL maintenance on critical facility infrastructure systems is fully scripted (detailed step-by-step).

- Experienced corporate engineers review ALL scripts prior to the work being done. Customers are advised in advance of critical maintenance activities

Effective testing and exercising of critical systems is also performed. These activities include:

- Rigorous testing, utilizing our on-site load banks to assure critical components such as UPS modules and engine-generators can reliably carry full rated load.

- Procedures that require full-load testing after significant repairs are made. (For example, if   UPS logic boards or power components are repaired or replaced, the unit will be fully tested before being placed back in service supplying critical customer loads.)

Power – Backup Generators

Our backup generators are tested in a comprehensive manner. Various scripted tests are conducted weekly, monthly (full load condition testing), quarterly, and annually, with all major components of the generator systems.

The fuel system is designed to support the generators under full load for a period of 48 hours. Redundant generators can power a facility for a minimum of two days. The facility has refueling contracts out to at least two contractors (contracts call for four hour response times) and the fueling is never allowed to drop below 75%.

Power Conditioning at the Datacenter

UPS, battery and diesel generators back up every power system. Power enters the facility from the local electric utility and is configured at 480 volt, 3-phase. The incoming power is fed into two busses, A and B, providing diverse power distribution to the cabinet areas. Back up power and power quality monitoring are provided through the UPS system, both for AC and DC power systems. DC power is produced onsite via the use of DC rectifiers. The AC power system is backed up under full load for up to 15 minutes. In the event of a power interruption, the backup batteries are a momentary source of electricity until the back up generators are brought online. Once the generator logic control system senses a power interruption, the generators are brought online in 7-9 seconds. Caterpillar diesel generator units power the

9

---

backup electrical power system. Fuel for the generators is supplied by at least two diverse suppliers and onsite fuel capacity provides for up to 48 hours of emergency power. Finally, dual AC and DC raceways with N+1 distribution are designed for a minimum 1.75kw per cabinet average draw. AC power delivery is via parallel redundant UPS systems.

Sub-Station Feeds

Our facilities receive multiple feeds from power utilities and distribute the power based on N+1 redundancy within each center. The fully redundant N+1 design is modular in nature, meaning that additional power system modules (battery strings, UPS modules, generators, etc.) can be added into the existing system should it become necessary to do so in order to maintain full redundancy.

Power Strips

Lore Systems supplies an 110V, 20 Amp, 10-receptacle horizontally mounted power strip free of charge with each 20 Amp circuit that is purchased. Furthermore, we have the ability to deliver virtually any denomination of power at an individual rack level, including 2 to 3 20 amp circuits to each rack as requested above. Conditioned AC power with two independent A & B power buses respectively is available to customers. When a customer utilizes an A and B feed, we can deliver 100% SLA on power availability. Lore works with customers to understand the exact requirements for the remotely managed power strips and come up with a mutually beneficial solution to meet this requirement. We have had great success meeting this requirement with many of our current customers.

UPS

Both AC and DC power are backed up by batteries that initiate automatically for up to (15) minutes of full-load operation using dual-redundant module Liebert UPS systems. Upon loss of utility power for more than two (2) seconds, emergency backup generators acquire the load for the duration of the utility outage.

10

Security

General Description

The physical security of the Lore Systems facilities is one of our highest operational priorities. Each facility utilizes an array of security equipment, techniques and procedures to control, monitor and record access to the facility, including customer cage areas. Some of the more visible security measures are described below.

24 x 7 Security Officers

We have the most senior level security officers from one of the world's largest and best-known security agencies. All officers undergo complete background/criminal checks and participate in forty hours of training.

Facility Access

Customers control access to each facility. No individual will gain access to the facility without having his or her visit previously scheduled. Moreover, we have the ability to track individuals. All physical access to the facility and customer cage is obtained via biometrics. Access can be scheduled through Lore Systems, providing tickets with audit logs for all access. Third party vendors will follow this same process and are able to gain access to the facility only with prior customer approval.

Biometric Hand Reader

Access to the front entrance of the facility is controlled through the use of a biometric hand reader combined with an assigned access code. A customer will have to pass through 5 readers to gain access to their cage.

Exterior Security

All points of ingress/egress are monitored by an intrusion detection system. Access points at the facility entrance are monitored and controlled by an access control subsystem that uses hand geometry readers interfaced with the security database. Authorized users are entered into the system and access events are archived for a period of time.

11

Interior Security

Interior points of ingress/egress are controlled by the access control subsystem. This includes entry through the mantrap and into each cage area. All areas of our centers are monitored and recorded using digitally recorded and archived closed circuit television (CCTV). The CCTV data is archived to disk for a minimum of 30 days. In addition, a video imaging subsystem stores digital photographs of individuals entering the facility. Bulletproof glass separates the security guard station from the lobby and Kevlar bullet-board surrounds the station window.

Annual Audits

Annual audits are conducted by the National Account Manager from our security contractor. These are comprehensive audits of technical and physical security. The goal of these audits is to pinpoint any security weak points and to address them. Results of these audits are analyzed by the site teams, the national security vendor account team, and the Lore Systems headquarters management teams.

Asset Tracking

Customers, as well as their vendors, contractors, and subcontractors often bring equipment into and remove equipment through the lobby.

To protect our customers', employees' and visitors' property, we have adopted the following asset tracking procedure to track property brought through the lobby at our centers

We record the following information for any piece of equipment valued at more than $1,000 that is transported through the mantrap. If the value of a component is in question and no purchase receipt is available, it will be appropriately logged.

- Description of major components
- Lore Systems Customer's Company Name
- Name, contact number, and signature of person

Also to protect customer assets, equipment removed [that was not brought in by that individual that day] must be listed on the individual's work visit ticket as equipment that may be removed. The description of the item[s] should be clear enough to identify the equipment, but does NOT need to include serial numbers, etc.

12

Physical Security (Alarms, Access, CCTV, Biometrics, Cages, Video)

The access control subsystem allows the distributed processing of stored information to allow authorized users inside the building and through the various doors within the facility. The reading devices are biometric hand geometry readers, which permit system users to identify themselves to the system and, based upon authorization, obtain access into a secure area.

Alarm Monitoring/Intrusion Protection

The alarm monitoring/intrusion detection subsystem monitors the status of various devices associated with the security system such as: alarm contacts, glass break detectors and motion detector tamper switches. If the status of any of these devices changes from their secure state, an alarm will be activated and displayed on the security system workstation and recorded on the system server's hard drive.

Video Imaging

The Video Imaging subsystem captures images that are stored on the security monitoring collection system. Video images are stored on archival media.

CCTV

The closed circuit television subsystem provides the display, control, recording and playback of live video from cameras throughout the facility. This system is integrated with the alarm monitoring/intrusion detection subsystem, so in the event of an alarm condition cameras can be called-up to record this event. Each camera is capable of accelerating digital recording during alarm conditions.

Audio Intercom & Two-Way Radio Subsystem

The audio intercom subsystem provides two-way communications between visitors to the facility and the Security Officer. The two-way radio subsystem provides communications between the front lobby Security Officer and the Patrol Officer.

Biometrics

All physical access to the facility and customer cage is obtained via a biometric hand scan. Access can be scheduled through our customer care system, providing tickets with audit logs for all access.

ID Requirements

All Lore employees are issued company ID cards, however, access to the datacenter facilities are strictly controlled through a multi-level security system that includes registration into the onsite security system that monitors access. This includes the enrollment and activation of the hand geometry readers throughout the centers.

To enter a center a customer must first present a valid picture I.D. We accept only pictured, government-issued forms of identification. Upon verification of identity, customers may be enrolled in our security systems, and with prior administrative access granted by the appropriate authorized customer administrator. Customers are required to always use the hand geometry readers.

Intrusion Testing

On a periodic basis our security contractor conducts intrusion testing. These drills are scheduled by the site manager on an as-needed basis with no advance warning to site staffs or security officers.

Security Personnel-Hiring/Training

Our centers employ the most senior level guards from one of the world's largest and best-known security agencies. All guards undergo complete background/criminal checks and participate in forty hours of program specific training.

Security Policies

In order to maintain a high-level of safety and security for Customers, customer data and hardware property around and within the facilities, Lore has established the following policies:

- Handling Emergencies
- Photographs in centers
- Asset Tracking
- Video Surveillance

Handling Emergencies

In the event of an emergency situation, e.g., fire, building evacuation, medical emergency, or drill, customers and other visitors on the premises will be required to follow instructions given by our on-site Site Manager or designee.

It is Lore Systems' intention to provide, at all times, a safe and secure working environment. Should a customer perceive any risk to their physical security or safety while in a center, the datacenter staff should be alerted. If a customer receives any telephone communication they perceive as threatening, our staff will provide forms for documenting the event. Maintaining safety and security in our centers is a prime goal of Equinix and Lore Systems.

Photography Inside Centers

Recording equipment is not permitted within the datacenter with the following exception.

Customers in private cages may submit a written request to photograph their cages and their equipment when they schedule a visit. Photographs may not be taken in shared cages. The Customer will be required to: 1) sign a non-disclosure agreement that stipulates any photos taken are for Customer internal purposes only, and will not be distributed or used in public marketing/promotional materials without prior written approval from Lore Systems, and 2) complete a "camera pass application".

The lobby security officer will supply both of these forms at the time of the customer's arrival, unless the customer's Lore Systems implementation or client relations manager has previously collected the completed non-disclosure agreement and delivered it to the lobby security officer for the customer.

A Lore Systems staff member will take the photographs with the customer's equipment, and will at all times control the equipment while it is inside the center.

Video Surveillance

All visitors to Lore datacenters should be aware that the centers are under constant video surveillance via over 2200 video cameras in each building.

LORE NAICS CODES

Codes	Descriptions
517911	Telecommunications Resellers
517919	All Other Telecommunications
518210	Data Processing, Hosting, and Related Services
519120	Libraries and Archives
519130	Internet Publishing and Broadcasting and Web Search Portals
519190	All Other Information Services
541511	Custom Computer Programming Services
541512	Computer Systems Design Services
541513	Computer Facilities Management Services
541519	Other Computer Related Services
541611	Administrative and General Management Consulting Services
541613	Marketing Consulting Services
541618	Other Management Consulting Services
541690	Other Scientific and Technical Consulting Services
541990	All Other Professional, Scientific, and Technical Services
551114	Corporate, Subsidiary, and Regional Managing Offices
561421	Telephone Answering Services
561422	Telemarketing Bureaus and Other Contact Centers

CONTRACTS & CERTIFICATIONS

	Maryland CATS II Master Contractor
	Certified MBE (minority business enterprise) by NMSDC (National Minority Supplier Development Council)

Lore Systems Contacts

S. Tien Wong
Chief Executive Officer
(703) 932-9191
twong@lore.net

Andrew Zaleski
Vice President & Director of Information Technology
(703) 402-0525
azaleski@lore.net

Oleg Gudym
Director, Business Development & Sales Engineering
(703) 855-1155
ogudym@lore.net

Lore Systems, Inc.
866.251.0167 toll free
703.542.2200 phone
703.542.1288 fax

www.lore.net